

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

**FILED**

**DEC 20 2016**

U.S. DISTRICT COURT  
EASTERN DISTRICT OF MO  
ST. LOUIS

**In the Matter of the Search of**  
Washington University in St. Louis  
#1 Brookings Drive, St. Louis, MO 63130  
Danforth University Center (DUC), Room 202;  
And all computers, computer hardware, wireless  
telephones, and Digital media located therein.

Case No. 4:16 MJ 6276 PLC

## APPLICATION FOR A SEARCH WARRANT

I, Jeffrey W. Wagner, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property: Washington University in St. Louis #1 Brookings Drive, St. Louis, MO 63130 Danforth University Center (DUC), Room 202; And all computers, computer hardware, wireless telephones, and Digital media located therein.

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENTS A & B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*

*Offense Description*

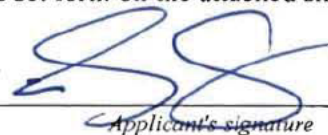
Title 18, U.S.C., Sections 2252 and 2252A

illegal importation, distribution and possession of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



*Applicant's signature*

Jeffrey W. Wagner, Special Agent, HSI

*Printed name and title*



*Judge's signature*

Honorable Patricia L. Cohen, U.S. Magistrate Judge

*Printed name and title*

AUSA: ROBERT F. LIVERGOOD

Sworn to before me and signed in my presence.

Date: December 20, 2016

City and State: St. Louis, MO

Washington University in St. Louis  
#1 Brookings Drive, St. Louis, MO 63130  
Danforth University Center (DUC), Room 202;  
And all computers, computer hardware, wireless telephones, and  
Digital media located therein.

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Jeffrey W. Wagner, being duly sworn, hereby depose and state:

1. I am a Special Agent of the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI, formerly the U.S. Immigration and Naturalization Service), currently assigned to the Office of Investigations in St. Louis, Missouri. I have been so employed for the past nineteen years. In that time period, I have received training in and have myself conducted numerous investigations of violations of Title 18, United States Code, Sections 2252 and 2252A (relating to the illegal importation, distribution, and possession of child pornography), as well as violations of Title 18, United States Code, Section 2422(b) (relating to the persuasion of coercion of a minor to engage in sexual activity). Specifically, during my employment as a Special Agent for HSI I have had the opportunity to conduct, coordinate and/or participate in numerous investigations relating to the sexual exploitation of children. I have also had the opportunity to observe and review numerous examples of child pornography in different forms of media including computer media, and have received training and instruction from experts in the field of investigation of child pornography. For approximately the past 2 ½ years, I have been assigned to the investigation of computer related crimes and the preservation of electronic evidence. My present responsibilities include the investigation of violations of Titles 8, 18, 19, 21 and 31 of the United States Code and related offenses.
2. This affidavit is in support of an application for a search warrant to search the premises known as Washington University in St. Louis, #1 Brookings Drive, St. Louis, MO 63130, Danforth University Center (DUC), Room 202 (hereafter known as Dean's Office), which is located in the Eastern District of Missouri. The Dean's Office is located on the campus of Washington University in St. Louis.
3. I am familiar with the information contained in this Affidavit based upon the investigation I have personally conducted, an interview with Justin CARROLL, and based on my conversations with other law enforcement officers involved in this investigation. In particular, I have received information unique to this investigation from Special Agent Austin Berrier



of the office of Homeland Security Investigations in Phoenix, Arizona.

4. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252, and 2252A are presently located at the Dean's Office, and within computer(s) and related peripherals, computer hardware and media, and wireless telephones found at that location. As a result of the investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Federal law, including 18 U.S.C. §§ 2252, and 2252A, more fully enumerated in the annexed Attachment A, are present in the Dean's Office.

#### **RELEVANT STATUTES**

5. This investigation concerns alleged violations of 18 U.S.C. Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors.
6. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).
7. Specifically, Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
8. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign

commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. Title 18, United States Code, Sections 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.
10. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
11. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
12. Title 18, United States Code, Sections 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means including by computer or mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

#### **DEFINITIONS**



13. The following definitions apply to this Affidavit and Attachment A to this Affidavit:

- a. "Child Pornography," as used herein, means any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8)(A) and (C).
- b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- c. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).
- d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
- e. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- f. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or

other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- g. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- i. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- j. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read



backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

- k. “Log Files” are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
- l. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- m. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- n. “Uniform Resource Locator” or “Universal Resource Locator” or “URL” is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- o. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any

means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- p. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- q. “Wireless telephone-” A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- r. “Peer-to-Peer (P2P)” – P2P is a distributed network architecture whereby network hosts share their resources (such as processing power and storage capacity) with other hosts without the need for a central managing device. Most Internet applications are *client-server*, whereby a host (e.g., an e-mail or Web user) obtains a service from another host (e.g., an e-mail or Web server). In a P2P environment, hosts communicate directly without the need of a server.



- s. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- t. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

### **COMPUTERS AND CHILD PORNOGRAPHY**

- 14. The information contained in this section is based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions.
- 15. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-based/ subscription-based Web sites to conduct business, allowing them to remain relatively anonymous. Child pornography is also traded through chat rooms and file sharing software.
- 16. The development of computers has also revolutionized the way in which child pornography collectors interact with, and sexually exploit, children. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. The development of computers has changed the methods used by child pornography collectors in the following ways:

- a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.
- b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online ("AOL") and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.
- c. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) Web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet



history and cache<sup>1</sup> to look for “footprints” of the Web sites and images accessed by the recipient.

- d. The computer’s capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 100 gigabytes or more are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the “scene of the crime”. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

### **THE INVESTIGATION**

17. In October 2015, HSI agents in Phoenix, Arizona, began conducting undercover operations on an Internet-based video conferencing application used by persons interested in exchanging child pornography and/or sexually abusing children. This application is hereinafter referred to as “Application A.”<sup>2</sup>
18. “Application A” is designed for video conferencing on multiple device formats. To use this application, a user downloads the application to a computer, mobile phone or other mobile device (*e.g.*, tablet) via direct download from the company’s website. Once downloaded and installed, the user is prompted to create an account. “Application A” users can invite others to an online meeting “room,” which is an online location associated

---

<sup>1</sup> “Cache” refers to text, image and graphic files sent to and temporarily stored by a user’s computer from a web site accessed by the user in order to allow the user speedier access to and interaction with that web site.

<sup>2</sup> The actual name of “Application A” is known to law enforcement. “Application A” remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as “Application A.”

with a 10-digit number where each user can see and interact with the other users.

19. When a user chooses to enter a specific meeting room, the user enters the 10-digit room number and enters the username that he wants to use on that specific occasion, which does not have to be the same as the account username. "Application A" does not require a certain number of characters for a particular username. Consequently, a user can create a name with a single special character, such as "#", or a single letter, such as "a."
20. During a meeting, users can show a live image or video of themselves to other users through the webcam feature. Users may also display the contents of their own computer desktops to the other users in the room. The ability to display their own computer desktops allows users to show videos and photos to other users in the room. "Application A" also allows users to send text messages visible to all of the users in the room, or private messages that are similar to instant messages sent between two users.
21. "Application A" permits users to conduct online video conferences for free for a limited number of minutes. Paid subscribers can conduct online video conferences for an unlimited amount of time. Some "Application A" users with a paid account permit their rooms to be accessed without a password such that anyone who knows the room number can enter and leave the room at any time.
22. "Application A" maintains IP address logs for each meeting room, which includes all of the IP addresses (and related usernames) for each user in a particular room on a specific day and the device that was used by each user. Each user's unique IP address is logged to reflect the time that particular user entered the room and the time the user exited the room. Users can enter and exit the room multiple times, thereby creating multiple sessions<sup>3</sup> within the logs of "Application A." In other words, if a room is open and active for one hour, and in that hour, a user enters the room, leaves the room, and then re-enters the room, the "Application A" IP log records would reflect two sessions for that specific user (entry/exit, followed by second entry) in the same room on that date.
23. On November 20, 2015, at approximately 3:21 pm Mountain Standard Time (MST), an HSI agent located in Phoenix, Arizona, acting in an undercover capacity (UCA) and using a device connected to the Internet, signed into an "Application A" user account and entered into "Application A" meeting

---

<sup>3</sup> As used herein, a session refers to a particular user's time in a specific "Application A" room.



room, "Meeting ID: 999-888-7321", without a password. The recorded session lasted until 4:40 pm MST.

24. A few of the usernames observed in the room included, "MOperv", "luzifer", "2 uk pervs", "meth-head ped", and "SCalPtyPvDad".
25. User "MOperv" was present in the room during the recording session from approximately 3:21 pm to 4:32 pm MST.
26. Within the room, the UCA observed that an "Application A" user displayed or streamed videos depicting child pornography, *i.e.*, visual depictions of a minor engaging in sexually explicit conduct, that were visible to users in the room. The UCA was able to record these child pornographic videos, and other activity and messages in the room, to an undercover device. The child pornographic videos included the following:
  - a. The first video scene recorded by the UCA occurred 39 seconds into the session and was being provided by participant "2 uk pervs". The video scene depicted an adult male engaging in anal sex on a prepubescent male, approximately 7-9 years old, while lying on a bed with white sheets and dark stripes.
  - b. From 3:38 pm to 4:27 pm MST a room participant using the username "luzifer" provided several video scenes depicting child pornography. Below are brief descriptions of three of the video scenes:
    - (1) A video scene of an adult male engaging in anal sex on a prepubescent male, age indeterminate. The adult male removes his penis from the boys' anus and ejaculates on the boys' genitals. The male is then seen rubbing his fingers on the boys' genitals.
    - (2) A video scene of a prepubescent male, approximately 6-8 years old with dark hair, performing oral sex on an adult male.
    - (3) A compilation of video scenes of several young males, most if not all, under 16 years of age, masturbating and ejaculating, showing close-ups of their anus, boys giving oral to other boys and inserting object(s) into their anus.
27. While recording the activity in the room, the following chat communications, both public (to "Everyone") and private (to and from the UCA) were observed (all times are in MST):
  - a. 3:46 pm: "MOperv" reaches out to the UCA and posts a private message asking "what are you into";

- b. 3:49 pm: The UCA responds to "MOperv" in a private message "yng  
bys...u?";
- c. 3:51 pm: The UCA posts a private message to "MOperv" asking "u in  
missouri?";
- d. 3:52 pm: "MOperv" posts a private message to the UCA responding  
"yes, are you?"; then: "ahh, US here"; and then: "MO";

(It should be noted that the webcam of "MOperv" was showing during  
this interaction and "MOperv" made motions with his arms, one hand  
going from his face downward out of view, as if he was typing a  
message, before the message was posted)

- e. 3:53 pm: The UCA posts a private message to "MOperv" responding  
"arizona";
- f. 3:53 pm: "MOperv" posts a private message to the UCA responding  
"bummer";
- g. 3:54 pm: The UCA posts a private message to "MOperv" asking "add  
me on skytpe";
- h. 3:54 pm: "MOperv" posts a private message to the UCA responding  
"jay.carr43 is my skype" "whats yours?";
- i. 3:55 pm: The UCA posts a private message to "MOperv" stating "just  
sent you a request...";
- j. 3:56 pm: The UCA posts a message to "Everyone" in the chat-room  
stating "hail luzifer!!!!", and "thx for sharing";
- k. 3:56 pm: "luzifer" posts to "Everyone" stating "great sons";
- l. 3:56 pm: "MOperv" posts to "Everyone" stating "thanks Luz"
- m. 4:05 pm: "MOperv" posts to "Everyone" stating "very nice";
- n. 4:26 pm: "luzifer" posts a message in the chat-room to "Everyone"  
stating "c ya later my sons..";
- o. 4:27 pm: "MOperv" posts a message in the chat-room to "Everyone"  
stating "hey thanks";



- p. 4:28 pm: "luzifer" posts a message in the chat-room to "Everyone" stating "enjoy ur yng ones 3:))"
28. During the same recorded session, numerous smaller windows appeared at the top of the screen showing some of the "Application A" meeting room participants' web cameras; in most cases, displaying in real time the "Application A" participant. One of the participants' cameras that was shown through the recorded session was that of user "MOperv," as denoted by the display name appearing in the lower left corner of the window. User "MOperv's" window streamed an image of a white male viewed primarily from the middle of the nose down to the bottom of his chest. "MOperv" was wearing a dark colored t-shirt. During a close-up of "MOperv" it appeared he had a white colored goatee. The room in which "MOperv" was located was viewable and had the following characteristics. A suspected fireplace was located to the far right of the screen. To the left of the fireplace is a glass door with white trim, a window is to the left of the door going to the end of the wall.
29. On November 23, 2015, at approximately 2:31 pm MST, an HSI agent located in Phoenix, Arizona, acting in an undercover capacity (UCA) and using a device connected to the Internet, signed into an "Application A" user account and entered into "Application A" meeting room, "Meeting ID: 999-888-7321", without a password. The UCA recorded session ended at 3:44 pm MST.
30. A few of the participant usernames observed in the meeting room included, "MOperv", "DADDYs faggot BA...", "Bare Perv", "satanazi//", and "s screen".
31. Participant "MOperv" was present in the room during the recording session from approximately 2:31 pm to 2:40 pm MST.
32. Within that room, the UCA observed that an "Application A" user displayed or streamed videos depicting child pornography, *i.e.*, visual depictions of a minor engaging in sexually explicit conduct, that were visible to users in the room. The UCA was able to record these child pornographic videos, and other activity and messages in the room, to an undercover device.
33. During "MOperv's" presence in the "Application A" meeting room from 2:31 pm to 2:35 pm MST, participant "s screen" played the following child pornographic scenes/videos for all to view. The following are descriptions are of just three of the scenes/videos:
- a. A video scene depicting an adult male laying on his back while a boy, approximately 5-8 years old, was engaged in oral sex on the adult male.

The boy was positioned so that he was laying on the adult males legs. The camera view is looking down at the boy from the left of the adult male. What appears to be the brown footboard of a bed is located behind the boy.

- b. A video scene titled "007.3gp" depicts a young boy, approximately 6-8 years old, sitting naked on the side of a bed, masturbating. After approximately seven seconds an adult male with dark hair leans in from the left of the screen and begins to perform oral sex on the boy. The bedspread is blue in color with light colored designs.
  - c. A video scene titled "01 hombre se coje a niño de 9 años.mp4" (according to the translation website "www.freetranslation.com" this translates in English to "01 man take a child of 9 years.mp4"). The scene depicts a young male with brown hair, possibly 7-9 years old, bending over a bed, lying on white pillows engaged in anal sex with an adult male. The adult male is filming the encounter from his point of view (looking down) and is wearing patterned underwear and a dark t-shirt. The scene then shows the encounter being filmed from a camera located to the left of the adult and boy. The adult male is seen engaging in anal sex on the boy. The bed is visible and has a headboard with vertical spindles. The adult's and boy's faces are not visible in the scene.
34. While recording the activity in the room, the following public chat communications to "Everyone" were observed (all times are in MST):
- a. 2:31 pm: "Bare Perv" posts a message in the chat-room to everyone stating "NOW WE PEEVIN"
  - b. 2:31 pm: "belower" posts to everyone ":P";
35. Participant "MOperv" window streamed an image of a white male viewed primarily from the middle of the nose down to the bottom of his chest. "MOperv" was wearing a light colored t-shirt. The room in which "MOperv" was located was viewable and appeared to be the same room described previously in paragraph 28.
36. On December 7, 2015, at approximately 9:50 am MST, an HSI agent located in Phoenix, Arizona, acting in an undercover capacity (UCA) and using a device connected to the Internet, signed into an "Application A" user account and entered into an "Application A" meeting room, "Meeting ID: 999-888-7321" without a password. The UCA recorded session lasted until to 10:09 am MST.



37. A few of the participant usernames observed in the meeting room included, "MOperv", "luzzifer", "Perv dad french", "Corrupted Daddy UK", and "meth-head ped".
38. Within the room, the UCA observed that an "Application A" user displayed or streamed videos depicting child pornography, i.e., visual depictions of a minor engaging in sexually explicit conduct, that were visible to users in the room. The UCA was able to record these child pornographic videos, and other activity and messages in the room, to an undercover device.
39. Participant "MOperv" was present in the room the entire time of the recording session.
40. During "MOperv's" presence in the "Application A" meeting room, participant "luzifer" played the following child pornographic scenes/videos for all to view. The following are descriptions of some of the scenes/videos:
  - a. A video scene depicting the following message in reverse image:

**"boybending"** (image blocked)

*"the art of remotely directing a boy on webcam, through typing text and displaying videos, to achieve a desired pose or behavior"*

*"use of coercion or blackmail is strictly forbidden"*
  - b. A video scene which consists of a compilation of several scenes quickly shown for a second. The scenes start out with the title "boybender" in reverse image at the top. A few of the scenes consist of a young preadolescent male being masturbated by the hand of someone not visible. Several scenes show preadolescent boys masturbating and ejaculating as well as inserting items in their anus.
41. While recording the activity in the room, the following public chat communications to "Everyone" were observed (all times are in MST):
  - a. 9:51 AM: "MOperv" posts a message in the chat-room to "Everyone" stating "sfuckin A. Hail Luz"
  - b. 9:52 AM: "luzifer" posts to everyone "hail bros" and then "amen"

- c. 9:52 AM: "MOperv" posts to everyone "amen bro"
  - d. 9:55 AM:
    - "Shaved Musclepig" posts to everyone "HAIL";
    - "pervvv" posts to everyone "its like ur dead and in heaven"  
"mmmmmmmmmm";
    - "pig italy" posts to everyone "666 extreme pedo"
  - e. 9:56 AM: "luzifer" posted to everyone "lil angels 2 play with"
  - f. 9:57 AM: "t" posted to everyone "need a lil boy :D"
  - g. 9:58 AM:
    - "A g" posted to everyone "u and me both";
    - "luzifer" posted to everyone "here we can get em alone"
  - h. 10:04 AM:
    - "pig italy" posted to everyone "I prefer boys";
    - "uk slammer" posted to everyone "i love watching women abuse kids" (a video of two women appearing to molest a young female is showing in the room at this time)
  - i. At 10:06 AM:
    - "XT1040" posted to everyone "pedo vids?";
    - "MOperv" posted to everyone "don't have any unfortunately. you?"  
and "just added you"
42. During the same recorded session, numerous smaller windows appeared at the top of the screen showing some of the "Application A" meeting room participants' web cameras; in most cases, displaying in real time the "Application A" participant. One of the participants' cameras that was shown through the recorded session was that of user "MOperv," as denoted by the display name appearing in the lower left corner of the window. User "MOperv's" window streamed an image of a white male viewed primarily from the middle of the nose down to the bottom of his chest. "MOperv" was wearing a light colored t-shirt. The room in which "MOperv" was located was viewable and appeared to be the same room described previously in paragraph 28.



43. On December 28, 2015, at approximately 2:04 pm MST, an HSI agent located in Phoenix, Arizona, acting in an undercover capacity (UCA) and using a device connected to the Internet, signed into an "Application A" user account and entered into an "Application A" meeting room "Meeting ID: 999-888-7321" without a password. The UCA recorded session lasted until to 3:02 pm MST.
44. A few of the usernames observed in the meeting room included, "MOperv", "skinpig666", "perv boi", and "prvin".
45. Participant "MOperv" was present in the room from 2:34 pm to 2:40 pm MST.
46. While recording the activity in the room, the following chat communications to "Everyone" were observed (all times are MST):
  - a. 2:34 pm: "sexpig47" posts a message in the chat-room to "Everyone" stating "no limizzz any 1"
  - b. 2:34 pm: "MOperv" posts a message in the chat-room to "Everyone" stating "no limits here"
  - c. 2:35 pm:
    - "bipedodad" posted in the chat-room to "Everyone" stating "any Southeast pedophiles?";
    - "strokinit" in the chat-room to "Everyone" stating "any boys n k9 ???"
  - d. 2:37 pm:
    - "twstdfkr" posted in the chat-room to "Everyone" stating "No limits Vry yng b and g";
    - "carlos ret" posted in the chat-room to "Everyone" stating "this pedo dick is hungry for boys ass"
47. On February 16, 2016, at approximately 10:44 am MST, an HSI agent located in Phoenix, Arizona, acting in an undercover capacity (UCA) and using a device connected to the Internet, signed into an "Application A" user account and entered into an "Application A" meeting room, "Meeting ID: 609-609-6009", without a password. The UCA recorded session lasted until to 10:59 pm MST.

48. A few of the usernames observed in the meeting room included, "MOperv", "uk perv", "2Poppers Perv Gay", "666" and "Perv Pig".
49. Within that room, the UCA observed that an "Application A" user displayed or streamed videos depicting child pornography, i.e., visual depictions of a minor engaging in sexually explicit conduct, that were visible to users in the room. The UCA was able to record these child pornographic videos, and other activity and messages in the room, to an undercover device.
50. During the same recorded session, numerous smaller windows appeared at the top of the screen showing some of the "Application A" meeting room participants' web cameras; in most cases, displaying in real time the "Application A" participant. One of the participants' cameras that was shown through the recorded session was that of user "MOperv," as denoted by the display name appearing in the lower left corner of the window. User "MOperv's" window streamed an image of a white male viewed primarily from the middle of the nose down to the bottom of his chest. "MOperv" was wearing a light colored t-shirt. The room in which "MOperv" was located was viewable and appeared to be the same room described previously in paragraph 28, but with a better view of the fireplace to the right of the screen. The mantle and trim of the fireplace is white in color with two candlesticks on top.
51. On February 16, 2016, at approximately 11:18 am MST, an HSI agent located in Phoenix, Arizona, acting in an undercover capacity (UCA) and using a device connected to the Internet, signed into an "Application A" user account and entered into an "Application A" meeting room, "Meeting ID: 609-609-6009", without a password. The UCA recorded session lasted until to 12:20 pm MST.
52. A few of the usernames observed in the meeting room included, "MOperv", "18yo Twink Perv in DFW", "Muscle666", "E" and "pigperv-spain".
53. Within that room, the UCA observed that an "Application A" user displayed or streamed videos depicting child pornography, i.e., visual depictions of a minor engaging in sexually explicit conduct, that were visible to users in the room. The UCA was able to record these child pornographic videos, and other activity and messages in the room, to an undercover device.
54. User "MOperv" was present in the room from 11:18 am to 11:58 am MST
55. During "MOperv's" presence in the "Application A" meeting room, participant "2Poppers Perv Gay" played the following child pornographic scene/video for all to view. The following is a description of the scene/video:



- a. At 11:22 am MST a video scene with the following alpha-numeric sequence at the top "1ef14754-3228-4fa3-a62a-d0c1..." was being broadcast in the room. The scene depicted an infant, gender unknown, under the age of 1, lying on its stomach on something dark with a white cloth next to it. An adult male, wearing a red shirt is engaged in anal sex on the infant. The infant is not moving during this scene.
56. While recording the activity in the room, the following public chat communications to "Everyone" were observed (all times in MST):
  - a. 11:22 am:
    - "Muscle666" posts a message in the chat-room to "Everyone" stating "snuff?"
    - "Ball" posts a message in the chat-room to "Everyone" stating "so hot"
  - b. 11:23 am:
    - "pigperv-spain" posts a message in the chat-room to "Everyone" stating "fuck yeah"
    - "Muscle666" posts a message in the chat-room to "Everyone" stating "ram that cok in HARD and break the kid"
  - c. 11:29 am: "boy" posts a message in the chat-room to "Everyone" stating "dead"
  - d. 11:31 am: "Muscle666" posts a message in the chat-room to "Everyone" stating "who's dead?, then "or who needs to be snuffed hehe >:)", then "no morals no mercy sick fuckers here?;
57. During the same recorded session, numerous smaller windows appeared at the top of the screen showing some of the "Application A" meeting room participants' web cameras; in most cases, displaying in real time the "Application A" participant. One of the participants' cameras that was shown through the recorded session was that of user "MOperv," as denoted by the display name appearing in the lower left corner of the window. User "MOperv's" window streamed an image of a white male viewed primarily from the middle of the nose down to the bottom of his chest. "MOperv" was wearing a light colored t-shirt. The room in which "MOperv" was located was viewable and appeared to be the same room described previously in paragraph 28.

58. On December 17, 2015, a U.S. Department of Justice Administrative Subpoena was served on "Application A" for subscriber and login information related to activity in the Application A room described above in paragraph 23 on November 20, 2015, paragraph 29 on November 23, 2015, and paragraph 36 on December 7, 2015. A review of the results revealed that a user of the subject display name "MOperv" logged in to this Application A room from the following IP address(es) on the dates and times specified; the times listed below are in UTC (Universal Time Coordinated):

IP	Join Time	Leave Time
99.47.206.0	11/20/2015 21:56	11/21/2015 1:08
99.47.206.0	11/23/2015 20:07	11/23/2015 21:40
99.47.206.0	12/7/2015 15:46	12/7/2015 17:38

59. On March 1, 2016, a U.S. Department of Justice Administrative Subpoena was served on "Application A" for subscriber and login information related to activity in the Application A room described above in paragraph 43 on December 28, 2015. A review of the results revealed that a user of the subject display name "MOperv" logged in to this Application A room from the following IP address(es) on the dates and times specified; the times listed below are in UTC:

IP	Join Time	Leave Time
99.47.206.0	12/28/2015 21:32	11/28/2015 21:39
99.47.206.0	12/28/2015 21:41	11/28/2015 21:52

60. On February 17, 2016, a U.S. Department of Justice Administrative Subpoena was served on "Application A" for subscriber and login information related to activity in the Application A room described above in paragraph 47 and 51 on February 16, 2016. A review of the results revealed that a user of the subject display name "MOperv" logged in to this Application A room from the following IP address(es) on the dates and times specified; the times listed below are in UTC:

IP	Join Time	Leave Time
99.47.206.0	2/16/2016 17:44	2/16/2016 18:58

61. A query of the American Registry for Internet Numbers (ARIN) online database revealed that IP address 99.47.206.0 is registered to AT&T Internet Services.
62. On March 22, 2016, a U.S. Department of Justice Administrative Subpoena was issued to AT&T Internet Services for subscriber information for the account associated with the IP address 99.47.206.0. A review of the results,



which were obtained on March 27, 2016, identified the following account holder as Cindy Carroll located at the address of 523 North and South Rd., St. Louis, MO 63130. The IP address was assigned to this user on August 18, 2015, and remained in effect until at least March 27, 2016.

63. On October 7, 2016, a Department of Homeland Security administrative summons was issued to AT&T Internet Services, requesting that AT&T identify the Internet account which had utilized IP address 99.47.206.0 to access the Internet from January 1, 2016, to the date of the Summons. A review of the results that were obtained on October 13, 2016, identified the following account holder as Cindy Carroll located at 523 North and South Rd., St. Louis, MO 63130. The IP address was assigned to this user on August 18, 2015, and remained in effect until at least October 13, 2016.
64. The records of the private database CLEAR showed that the residents of 523 North and South Rd., St. Louis, MO 63130, to be Justin X. CARROLL and Cecelia K. Carroll.
65. The records of Ameren Corporation, obtained on November 30, 2016, reveal that the responsible party for electrical service at 523 North and South Rd., St. Louis, MO 63130, is Justin X. CARROLL. The electrical service is currently active in that name, and began on July 31, 2013.
66. On October 13, 2016, at approximately 9:57 am MST, an HSI agent located in Phoenix, Arizona, acting in an undercover capacity (UCA) and using a device connected to the Internet, signed into an "Application A" user account and entered into an "Application A" meeting room, "Meeting ID: 494-949-4949", without a password. The UCA recorded session lasted until 11:14 am MST.
67. A few of the usernames observed in the meeting room included, "MOperv", "pd bro", "bbyfkr", "dadxxx" and "I fuk boys".
68. Within that room, the UCA observed that an "Application A" user displayed or streamed videos depicting child pornography, i.e., visual depictions of a minor engaging in sexually explicit conduct, that were visible to users in the room. The UCA was able to record these child pornographic videos, and other activity and messages in the room, to an undercover device.
69. During the same recorded session, numerous smaller windows appeared at the top of the screen showing some of the "Application A" meeting room participants' web cameras; in most cases, displaying in real time the "Application A" participant. One of the participants' cameras that were shown through the recorded session was that of user "MOperv," as denoted by the display name appearing in the lower left corner of the window. User

“MOperv’s” window streamed from a webcam, pointed down. The webcam appears to be located on top of a computer screen. The video shown is of the lower portion of a computer screen on top of a brown piece of furniture. A window box is open on the computer displaying what looks to be a video but due to the angle of the camera the video is not describable.

70. On October 13, 2016, a U.S. Department of Justice Administrative Subpoena was served on “Application A” for subscriber and login information related to activity in the Application A room described above in paragraph 66 on October 13, 2016. A review of the results revealed that a user of the subject display name “MOperv” logged in to this Application A room from the following IP address(es) on the dates and times specified; the times listed below are in UTC

IP	Join Time	Leave Time
128.252.158.159	10/13/2016 18:11	10/13/2016 18:14

71. A query of the American Registry for Internet Numbers (ARIN) online database revealed that IP address 128.252.158.159 is registered to Washington University located at 1 Brookings Drive, St. Louis, MO 63130.
72. Additional information provided by “Application A” showed that “MOperv” accessed “Application A” on November 23, 2015 from the IP Address 128.252.48.27 from 23:44 to 05:00 UTC.
73. A query of the American Registry for Internet Numbers (ARIN) online database revealed that IP address 128.252.48.27 is registered to Washington University located at 1 Brookings Drive, St. Louis, MO 63130.
74. An internet search of the name Justin CARROLL revealed a February 23, 2016 posting on the Washington University in St. Louis Athletics webpage naming Justin X. CARROLL the interim Director of Athletics. The posting stated that CARROLL has served as Dean of Students since 1992, and in 1997, was named Assistant Vice Chancellor and Dean of Students.
75. On December 20, 2016, a federal search warrant was executed on 523 North and South Rd., St. Louis, MO 63130 based on information provided in this affidavit.
76. The resident of the home, Justin CARROLL, agreed to answer questions posed by your Affiant. CARROLL stated that he was aware of “Application A”, and it was currently present on his laptop and cellular phone.



77. CARROLL said he had a username on "Application A", "JMO". When CARROLL was asked about the username "MOperv", he responded that was also one of his usernames.
78. During an interview with Cindy King-Carroll, CARROLL'S wife, King-Carroll was shown screenshots taken from the videos provided by HSI Phoenix of "MOperv" in one or more of the "Application A" meeting rooms showing child pornography. King-Carroll was not shown any depictions of child pornography, only screenshots of CARROLL or the room he was in while accessing "Application A"
79. While looking at the screenshots, King-Carroll positively identified the images of "MOperv" as her husband CARROLL. King-Carroll also positively identified the room in which CARROLL was in while accessing "Application A", as a room in their residence.
80. CARROLL stated that he used the username "MOperv" to access "Application A" from his residence and his "work". When CARROLL accessed "Application A" from "work" using the username "MOperv", he did it mostly in the "evenings", or "late".
81. CARROLL stated he believes "Application A" is downloaded on his computer at work.
82. CARROLL stated that he currently holds two positions at Washington University and occupies two offices. CARROLL has an office as the Associate Vice Chancellor of Students / Dean of Students, and an office as the Interim Athletic Director.
83. Washington University Police Lt. Frank Selvaggio, provided the address of the Dean's Office as Washington University in St. Louis, #1 Brookings Drive, St. Louis, MO 63130, Danforth University Center (DUC), Room 202.

**CHARACTERISTICS OF INDIVIDUALS WHO RECEIVE AND  
COLLECT IMAGES OF CHILD PORNOGRAPHY**

84. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:
  - a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing

children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

- b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Collectors of child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica,<sup>4</sup> and videotapes for many years.
- d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the collector to view the collection, which is valued highly.
- e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

---

<sup>4</sup> “Child erotica,” as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.



- f. Collectors of child pornography prefer to have continuous access to their collection of child pornography. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
85. Based upon the conduct of individuals involved in the collection of child pornography set forth above, namely, that they tend to maintain their collections at a secure, private location for long periods of time, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the premises described previously herein, known as, and the computers and computer media located therein.

### **SEIZURE OF EQUIPMENT AND DATA**

86. Based upon my knowledge, training and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:
- a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process may take weeks or months, depending on the volume of data stored and it would be impractical to attempt this kind of data analysis on-site.
  - b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files.

Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

87. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such-- or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readable, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.
88. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was



downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

89. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have spoken, I am aware that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize most or all of a computer system's input/output peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPU) and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.
90. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

#### **COMPUTER EXAMINATION METHODOLOGY TO BE EMPLOYED**

91. The examination procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include

the following techniques (the following is a non-exclusive list, as other examination procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

### CONCLUSION

92. Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A, which, among other things, make it a federal crime for any person to knowingly access with the intent to view, possess and/or receive child pornography, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment A of this Affidavit, are located at Washington University in St. Louis, #1 Brookings Drive, St. Louis, MO 63130, Danforth University Center (DUC), Room 202, and any computers, computer media, or wireless telephones therein, and more fully described herein. Your Affiant requests authority to seize such material, specifically, that the Court issue a search warrant for these premises and all computers, computer hardware and



media, and wireless telephones therein.

## ATTACHMENT A

### LIST OF ITEMS TO BE SEIZED

1. Computer(s), computer hardware, wireless telephones, computer software, computer related documentation, computer media (including any and all web cameras), computer passwords and data security devices, wireless phones, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, or information pertaining to an interest in child pornography.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, file sharing software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the online accessing with the intent to view, possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8)(A) or (C) or to the online accessing with the intent to view, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2)(A).
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8)(A) or (C), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2)(A).
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by Justin CARROLL by use of the computer or by other means for the purpose of producing, distributing or receiving child pornography as defined in 18 U.S.C. 2256(8)(A) or (C) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. 2256(2)(A).
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce



by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8)(A) or (C) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the online accessing with the intent to view, receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8)(A) or (C) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A).
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all visual depictions of minors under the age of eighteen years engaged in sexually explicit conduct.
13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium

(including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8)(A) or (C) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A).

14. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors under the age of eighteen years visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A).



**ATTACHMENT B**

Driver's License Information

